David S. Casey, Jr., SBN 060768
dcasey@cglaw.com
Gayle M. Blatt, SBN 122048
gmb@cglaw.com
Jeremy Robinson, SBN 188325
jrobinson@cglaw.com
P. Camille Guerra, SBN 326546
camille@cglaw.com
Catherine M. McBain, SBN 303911
kmcbain@cglaw.com
CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CHRISTINA PRICE, individually and on behalf of herself and all other persons similarly situated,

Plaintiff,

v.

ACCELLION, INC.,

Defendant.

CASE NO.

Class Action Complaint for Damages

Demand for Jury Trial

1. Plaintiff Christina Price brings this class action against Defendant Accellion, Inc., a California-based cloud service provider, for its failure to properly secure and safeguard personally identifiable information that was stored on or shared on its "Accellion FTA" file transfer service. The Class includes all residents of the United States whose data was stolen from Accellion in the data breach or breaches during December 2020 and January 2021 (collectively, the "Data Breach.")

2. Defendant Accellion touts that its Accellion FTA service "helps worldwide

enterprises transfer large and sensitive files securely using a 100% private cloud, on-premise or hosted."[1]

3. In reality, Accellion's FTA is an obsolete 20 year old technology riddled with security vulnerabilities. Those vulnerabilities were exploited by hackers in December 2020 when they infiltrated Accellion's system and stole a huge number of names, social security numbers, driver's license or state identification numbers, dates of birth, bank account numbers, and in some cases, medical information, including prescription information and diagnoses, and salary information (collectively, "personally identifiable information" or "PII").[2] In addition, there are reports that the breach continued into January 2021 after Accellion failed to successfully update its security systems.

4. The list of major institutions whose data was stolen from this Data Breach continues grow. So far, entities as diverse as the Kroger Company, law firm Jones Day, the State of Washington, the University of Colorado, the Reserve Bank of New Zealand, Transport for New South Wales, the Australian Securities and Investments Commission, and Singapore Telecommunications have all announced major data thefts from Accellion's FTA service.

5. Accellion knew that its customers included public and private business enterprises and that these customers would rely on Accellion's representations "to transfer large and sensitive files," including sensitive files containing PII, and that it was important and necessary that such large and sensitive files be transferred "securely."

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and

---

[1] *See* https://www.accellion.com/products/fta/ (last visited Feb. 24, 2021).

[2] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. It includes, but is not limited to, all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, medical information, etc.).

Class Members' PII, Accellion assumed legal and equitable duties to those individuals.

7. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers, medical record information, and other PII that is difficult or impossible to change.

8. Indeed, security company Mandiant reported that since the breach, some victims have reported receiving extortion emails from groups claiming to be associated with the breach.

9. Plaintiff brings this action on behalf of all persons whose PII was compromised because of Defendant's failures to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) effectively secure hardware and/or software containing protected PII using reasonable and effective security.

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) actual instances of identity theft or fraud; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued increased risk to their PII.

11. Defendant disregarded the rights of Plaintiff and Class Members by recklessly, or negligently failing to take adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow required and appropriate protocols, policies, and procedures regarding the encryption of data. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third parties. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to

injunctive and other equitable relief.

THE PARTIES

12. Plaintiff Christina Price is a citizen and resident of the State of Georgia.

13. Defendant Accellion, Inc., is a corporation organized under the laws of Delaware, headquartered at 1804 Embarcadero Road, Suite 200, Palo Alto, California.

14. All of Plaintiff's claims are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

15. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

16. This Court has personal jurisdiction over Defendant because it maintains its principal places of business in this District, is registered to conduct business in California, and has sufficient minimum contacts with California.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this District and a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District.

18. Application of California law to this dispute is proper because Accellion's headquarters are in California, the decisions or actions that gave rise to the underlying facts at issue in this Complaint were presumably made or taken in California, and the misconduct emanated from California. Additionally, Defendant's employees involved in the misconduct are presumably located at Defendant's headquarters.

FACTUAL ALLEGATIONS

19. Accellion was founded in 1999 and originally focused on providing distributed file storage management and backup technology. Beginning in 2001, the company moved its headquarters to Palo Alto, CA and concentrated its business on file transfer technology.

20. Accellion FTA advertised itself as allowing users to "transfer large and sensitive files securely."

21. Prior to December 2020, Accellion knew its FTA was severely outdated and had been privately notified by several security firms of major bugs or security flaws in the FTA. Yet, Accellion did not retire the FTA even though it had developed newer and better services.

22. In or about December 2020, and continuing into January 2021, Accellion's FTA product was subject to an SQL injection vulnerability Security Incident which compromised a range of clients including Kroger.

23. Accellion FTA was used to transfer some of Plaintiff's and Class Members sensitive and confidential PII, including names, social security numbers, driver's license or state identification numbers, and other personal identifiable information, which can be used to commit financial crimes including identity theft.

24. Accellion claims it notified its FTA customers of the Data Breach on December 23, 2020.

25. On or around January 15, 2021, the Reserve Bank of New Zealand announced that it was one of the Accellion FTA customers affected by the Data Breach.

26. On or around January 25, 2021, The Australian Securities and Investments Commission ("ASIC") announced that it was one of the Accellion FTA customers affected by the Data Breach.

27. On February 19, 2021, Kroger announced it was also impacted by the Accellion data breach. Kroger noted that it discontinued use of Accellion's services after it was informed of the effect of the incident on Jan. 23, 2021. The retailer said that, at the time, it also reported the incident to federal law enforcement and launched its own forensic inquiry to review the potential scope and impact of the incident.

28. Over the subsequent weeks many other organizations announced they were also victims of the Accellion data breach.

29. On February 24, 2021, the cybersecurity authorities of Australia, New

Zealand, Singapore, the United Kingdom, and the United States released Joint Cybersecurity Advisory AA21-055A: Exploitation of Accellion File Transfer Appliance. It states that "cyber actors worldwide have exploited vulnerabilities in Accellion File Transfer Appliance to attack multiple federal, and state, local, tribal, and territorial government organizations as well as private industry organizations in the medical, legal, telecommunications, finance, and energy fields. In some instances, the attacker extorted money from victim organizations to prevent public release of information exfiltrated from a compromised Accellion appliance."

30. The release also notes there have been ongoing extortion attempts of victims of the Data Breach by hackers and other bad actors.

31. Accellion could have prevented this Data Breach by properly securing and encrypting Plaintiff's and Class Members' PII and keeping its services and products up to date.

32. Defendant's failure to safeguard Plaintiff's and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data.

33. The ramifications of Defendant's failure to keep secure Plaintiff's and Class Members' PII are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years. Plaintiff's and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

34. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

35. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends,

and colleagues of the original victim.

36. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

37. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

38. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

39. For example, The United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name. See Government Accountability Office, Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007), available at http://www.gao.gov/assets/270/262899.pdf (last visited September 24, 2020). The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name." Id.

40. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number or

government-issued identification number, name, and date of birth.

41. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."

PLAINTIFF'S CIRCUMSTANCES

42. Plaintiff Christina Price is a former employee of Kroger where she was employed as a customer service manager approximately four years ago. As a condition of employment, Plaintiff provided Kroger with her Personally Identifiable Information.

43. On or around February 23, 2021, Plaintiff received a Notice of Data Breach from Kroger. The Notice referenced a "security incident affecting Accellion, which was used by the Kroger Family of Companies…for secure file transfers."[3] Further, the Notice states that "Accellion has confirmed that an unauthorized person gained access to certain Kroger Family of Companies files by exploiting a vulnerability in Accellion's file transfer service."

44. The notice states that they "believe impacted information may include names, email address and other contact information, date of birth, Social Security number, and for former associates, may have also included certain salary information such as net and gross pay and withholdings."

45. As a result of learning of the Data Breach, Plaintiff spent time dealing with the consequences of it, including spending time verifying the legitimacy of the news reports of the Data Breach, exploring and signing up for credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

46. Additionally, Plaintiff is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

[3] Kroger Notice of Data Breach dated February 19, 2021

47. Plaintiff stores any documents containing her PII in a safe and secure location or destroys the documents, including taking them to a local UPS store to be shredded.

48. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

49. Plaintiff has suffered the above and other imminent and impending injury from the substantially increased risk of fraud, identity theft, and misuse of her PII, especially her Social Security number.

50. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

51. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and the following proposed Class:

> All persons in the United States whose PII was stolen in the Data Breach of Accellion's FTA in December 2020 and January 2021.

52. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of Accellion; ; and any judge to whom this case is assigned, and members of the judge's staff.

53. **Numerosity:** Members of the proposed class likely number in the thousands and are thus too numerous to practically join in a single action.

54. **Commonality and Predominance:** Common questions of law and fact exist as to all proposed class members and predominate over questions affecting only individual class members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's inadequate data security measures were a cause of the Data Breach;

c. Whether Defendant owed a legal duty to Plaintiff and the other Class members to

exercise due care in collecting, storing, and safeguarding their PII;

d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff and the other class members to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Plaintiff and the Class have suffered benefit of the bargain losses because of the Data Breach;

g. Whether Defendant's conduct violated Cal. Bus. & Prof. Code § 17200 et seq.;

i. Whether Plaintiff and the other class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

j. Whether Plaintiff and the other class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

55. These issues not only predominate, they are also matters appropriate for issue certification under Rule 23(c)(4).

56. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

57. **Typicality:** Plaintiff's claims are typical of the claims of the other Class members because, among other things, Plaintiff and the other Class members were injured through the substantially uniform misconduct by Defendant. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all other class members, and there are no defenses that are unique to Plaintiff.

58. **Adequacy of Representation:** Plaintiff is an adequate representative of the class because her interests do not conflict with the interests of the other class members she seeks to represent; she has retained counsel competent and experienced in complex

class action litigation, and Plaintiff will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiff and her counsel.

59. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for class members to individually seek redress for Defendant's wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION

Unlawful, Unfair, and Fraudulent Business Practices

Cal. Bus. & Prof. Code § 17200, et seq.

(on behalf of Plaintiff and the Class)

60. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

61. Defendant Accellion violated, and continues to violate, California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200, et seq., which prohibits unlawful, unfair, or fraudulent business acts or practices.

62. Defendant's conduct, as alleged above, is unlawful because it violates the Confidentiality of Medical Information Act, Civil Code § 56, *et seq.* (the "CMIA"), the Customer Records Act, Civ. Code § 1798.80, *et seq.*, (the "CRA") the Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq.* (the "CCPA"), Section 5 of the Federal Trade Commission Act, and other state data security laws.

63. Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, both by affirmative conduct and by omission, the safety of its computer systems, specifically the security thereof, and its ability to safely store Plaintiff's and all Class members' PII.

64. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to timely notify Plaintiff and all Class members of the Data Breach.

65. Defendant also violated California Civil Code § 1798.81.5(b) in that it failed to maintain reasonable security procedures and practices.

66. Defendant additionally violated California Civil Code section 1798.150 by failing to maintain and implement reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and the Class's unredacted and unencrypted PII.

67. If Defendant had complied with these legal requirements, Plaintiff and all Class members would not have suffered the damages related to the Data Breach.

68. Defendant's conduct is an unfair practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes failing to adequately ensure the privacy, confidentiality, and security of PII entrusted to it, having grossly outdated systems and programs, and failing to have basic data security measures in place.

69. Defendant also engaged in unfair business practices under the "tethering test." Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature

to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

70. Instead, the PII of Plaintiff and the Class, including their Social Security numbers, driver's license information, and other information, were made accessible by Defendant to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violates the policies underlying the laws set out in the prior paragraph.

71. The harm caused by Defendant's unfair practices outweighs any potential benefits from those practices. Further, there were reasonable alternatives available to Defendant to further their legitimate business interests.

72. Plaintiff and all Class members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. Among other things, Plaintiff and the Class members did not receive the benefit of their bargain with Defendant in that the services they received and paid for should have included keeping their PII encrypted and secure and did not. In addition, Plaintiff's and all Class members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value.

73. As a result of Defendant's violations of the UCL, Plaintiff and the Classes are entitled to restitution and other equitable relief.

SECOND CAUSE OF ACTION

Negligence

(on behalf of Plaintiff and the Class)

74. Plaintiff repeats, re-alleges and incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

75. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care

in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiff's and Class members' PII in Defendant's possession was adequately secured and protected, and encrypting the PII.

76. Defendant owed a duty of care to Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that its systems and networks adequately protected the PII of its patients.

77. Defendant owed a duty of care to Plaintiff and members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII of its current and former patients and the critical importance of adequately securing such information.

78. Defendant breached these duties by failing to adequately safeguard the privacy, confidentiality, and security of Plaintiff's and Class members' personal information and documents. Through Defendant's acts and omissions, including Defendant's failure to provide adequate security and its failure to protect Plaintiff's and Class members' PII from being foreseeably accessed, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class members during the time it was within Defendant's possession or control.

79. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the benefit of their bargain with Defendant; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and

recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that the Court enter a judgment awarding the following relief:

a. An order certifying the proposed Class, and appointing Plaintiff's counsel to represent the Class;

b. An order awarding Plaintiff and the Class members damages, restitution, disgorgement, and/or any other form of monetary relief provided by law;

c. An order declaring Defendant's conduct to be unlawful;

d. An order enjoining Defendant's conduct and requiring Defendant to implement proper data security policies and practices; specifically:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiff and the Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class

members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and the Class members' PII;

v. prohibiting Defendant from maintaining Plaintiff's and the Class members' PII on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and the Class members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xviii. requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected;

xix. requiring Defendant to disclose any future data breaches in a timely and accurate manner;

xx. requiring Defendant to implement multi-factor authentication requirements;

xxi. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxii. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class members.

e. An order awarding Plaintiff and the Class's reasonable costs of suit;

f. An order awarding Plaintiff and the Class pre-judgment and post-judgment interest as allowed under the law; and

g. An order awarding such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of themselves and the proposed Class, hereby demand a trial by jury as to all matters so triable.

Dated: February 26, 2021

/s/Gayle M. Blatt
GAYLE M. BLATT
Attorneys for Plaintiff

CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232